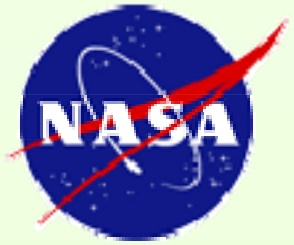


Overview of NASA's Certification-Relevant Research

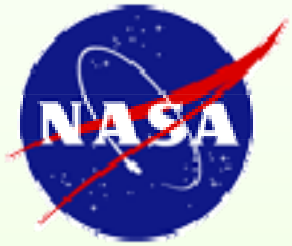
Kelly J. Hayhurst

NASA Langley Research Center

Presented at the 2005 FAA/NASA Software and Complex Electronic Hardware Conference

Norfolk, Virginia

July 26-28, 2005



Overview of NASA *Langley's* Certification-Relevant Research

Kelly J. Hayhurst

NASA Langley Research Center

Presented at the 2005 FAA/NASA Software and Complex Electronic Hardware Conference

Norfolk, Virginia

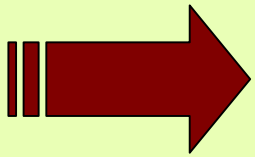
July 26-28, 2005

If you build it, they will come

- we'd like to do a little better…

Why is NASA here?

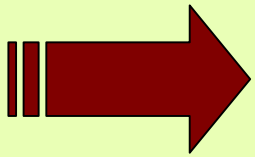
To foster a better relationship with you



To build a research program to meet your needs

Why is NASA here?

To foster a better relationship with you



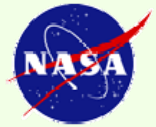
To build a research program to meet your needs

- *and better coordinate certification-relevant research within NASA, while we're at it*

Outline

- A view from within NASA
  - past & present research activities
  - things to come
- A view from the world around us
  - common goals
  - common trends
  - common problems
- A view of where we would like to go

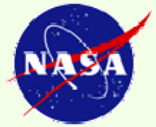
Past Work within (or supported by) NASA Langley



- Participation in RTCA/SC-167 (that created DO-178B)
- DO-178B case study*
- Streamlining Software Aspects of Certification*
- Participation in RTCA/SC-190, *Software Application Guidelines For RTCA DO-178B/ED-12b (Software)*
- Modified Condition/Decision Coverage (MC/DC) Research & Tutorial*
  - with Rockwell Collins & Boeing
- Object-Oriented Technology in Aviation (OOTiA) Workshops*
- Verification and validation methods for neural networks
  - with Barron Associates & Goodrich Aerospace
- Software Verification Tools Assessment Study*
  - with Boeing

**sponsored by FAA*

Current Work within (or supported by) NASA Langley



- **Participation in**
  - RTCA/SC-200, *Integrated Modular Avionics*
  - RTCA/SC-205, *Software Considerations in Aeronautical Systems*
- **Aviation Accident Analysis**
  - causal analysis of previous accidents (*Wed. 4 pm*)
  - enhanced safety-cases (*Thu. 10 am*)
- **Formal Methods**
  - air traffic management
  - fault-tolerant architectures (SPIDER) (*Wed. 1 pm*)
  - model-based development (*Thu. 8 am*)
  - operating systems (*Thu. 8 am*)
  - requirements engineering, situated formalisms & assured reconfiguration (*Thu. 10 am*)

Current Work within NASA

- **Application of DO-178B in research software systems**
  - **Airborne Research Integrated Experiments System (ARIES – B757)**

- **Work at other NASA centers**
  - **adaptive flight control systems @ NASA Ames & Dryden (Thu. 8:45 am)**
  - **software certificate management (new) & program synthesis @ NASA Ames**
  - **programmable logic devices @ NASA Goddard (Wed. 1 pm)**
  - **multifunction, multimode digital avionics (Software Radio) @ NASA Glenn (just starting)**

Characteristics of Past & Present Work

- Driven from
  - specific FAA requests
  - individual researcher interests
  - some programmatic support
    - Aviation Safety Program
- Spotty coverage of civil certification-related problems
- No intra-agency coordination
- Ad hoc industry involvement
  - no effective plan for research-industry cooperation

No unifying goals or strategy

Things to Come

On a Shorter Horizon…

NASA's Aeronautics Blueprint defines 52 technology solutions in a research agenda for developing an on-demand, on-time, efficient, environmentally friendly, air transportation system

Revolutionary Vehicles	Aerospace System	Security & Safety
"Refuse to Crash" flight controls	National Airspace Management	Network intrusion prevention
Self-healing systems	All-weather situational awareness	Recoverable computers
Synthetic vision	Smart non-towered airports	Secure communications
Central "nervous system"	Secure networked communications	Real-time passenger threat assessment
Intelligent combustors	Integrated decision-support tools	Remote audio & visual links

VISION 100 – Century of Aviation Reauthorization Act, Public Law 108-176

- **To establish in the FAA a Joint Planning and Development Office to manage work for the Next Generation Air Transportation System**
  - **includes NASA, the Departments of Commerce, Defense, Homeland Security, Transportation, the White House Office of Science and Technology Policy, industry & academia**
- **Responsibilities include -**
  - **creating and carrying out an integrated plan for a Next Generation Air Transportation System**
    - and creating a transition plan for the implementation of that system
  - **coordinating research programs to achieve the goal**
  - **coordinating the development and utilization of new technologies to ensure that when available, they may be used to their fullest potential**
  - **facilitating technology transfer from research programs to Federal agencies with operational responsibilities and to the private sector**

The JPDO plan

- **Integrated National Plan for the Next Generation Air Transportation System (Dec. 2004) includes**
  - **establishing an agile air traffic management system**
    - **new technologies that promote capacity growth & increase efficiency**
    - **optimizing allocation of functions between automation and humans & between ground and air vehicles**
    - **providing more routine operations in adverse weather**
  - **establishing user-specific situational awareness**
    - **comprehensive awareness of the air transportation system, including real-time notification of changes**
  - **developing a system-wide capability to reduce weather impacts**
  - **integrating surveillance and intent information, including anomaly detection and conformance monitoring**

Unconventional things are coming, too…

… Sooner than you may think

Access 5 is a NASA-led program, with DoD & FAA

- **AeroVironment, Aurora Flight Sciences, Boeing, General Atomics, Lockheed Martin, and Northrop Grumman**

- **Purpose: propose acceptable policy & guidance to facilitate operation of unmanned aircraft routinely, safely, and reliably in the National Airspace System**

- **RTCA/SC-203 Unmanned Aircraft Systems**
  - **developing Minimum Aviation System Performance Standards (MASPS) for unmanned aircraft**

- **Software & complex electronic hardware issues:**
  - **What should design assurance requirements be for systems where automation (*not a pilot*) have the ultimate authority?**

Common Desire

- Lots and lots of unprecedented levels of automation

Common Trends

Abstraction

- Model-based development
- Object and aspect-oriented programming

Automation

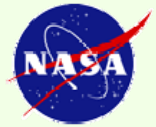
- Translations
- Testing
- Analysis

Collaboration

- At the aircraft system level
  - from federated to integrated systems
- At the airspace management level

- **So much is changing – *but some things remain the same…***

Fundamental problems



- How to efficiently, accurately, and completely determine and specify requirements
- How to efficiently, accurately, and completely determine and specify system safety properties
- How to best partition requirements and safety properties among software, hardware, and humans
- How to efficiently verify that a software system satisfies all its requirements and maintains all its safety properties
- How to demonstrate to others, such as certification authorities, that all necessary verification and validation has been completed
- When accidents do occur, how to effectively diagnose the software contributions to the accidents, so that future systems will not be susceptible to similar accidents.
- …

Common Outcomes

- from Aviation Week

"Software is both the friend and foe of aerospace. It provides enormous flexibility, but ensnares with a complexity that can lead to programmatic and physical disaster. "

[ref. Dornheim, *Codes Gone Awry*, Aviation Week & Space Technology, Feb 28, 2005]

- from the Center for National Software Studies

"… Significant advances have been made and continue to be made in software technology, tools and practices. That was the good news. The bad news is that in the same period of time, the growth in pervasiveness and complexity of software has significantly outpaced that progress..."

[ref. Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness, May 2005]

In the Military, too

- from Aviation Week

"With the threat of continued software problems derailing U.S. Air Force plans for the F/A-22 stealth fighter, prime contractor Lockheed Martin has devised a way to gradually overcome long-standing glitches that have led to repeated crashes of onboard computers."… "*the greatest challenge in the F/A-22 development program is one of software integration, which has resulted in a software instability* …"

[ref. Hall, *Code Red Emergency*, Aviation Week & Space Technology, Jun. 9, 2003]

- from the Colonel

"Software V&V is the Achilles' heel to fielding new flight control systems."

"We don't have the right toolset to get advanced systems into the field. We want to develop systems that we know up front are certifiable. "

[ref. Col. Michael Leahy, Flight Critical Systems Software Initiative (FCSSI) workshop, July 2004]

Common Characteristics

- Desire for increased capabilities and collaboration in vehicle technologies and air traffic management
  - On the civilian side: to give us on-demand, on-time, efficient, environmentally friendly, air transportation
  - On the military side: to give us advanced capabilities with reduced loss of life
  - with reduced life cycle cost
  - with reduced time from concept to the field
- But, lots of difficulties getting there

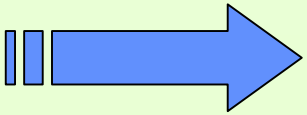
Unifying goals – but few tactics

Where we like to go from here

It seems logical that research would be beneficial

Desired Characteristics of Future Work

- Driven from
  - realistic assessment of actual needs
- Unifying goals and strategy
- Targeted coverage of critical needs for which we have expertise to handle
- Coordinated industry involvement
- Agency/Program support

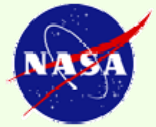


Aviation Safety & Security Program (AvSSP) Phase II

Software Safety & Certification

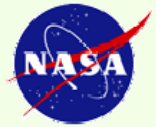
- FY '06 is a transitional year in AvSSP
  - gearing towards a 5-year research program, starting in FY '07
- To help define what that program should be, we want to
  - characterize the state-of-the-practice in software design and certification
    - identify current barriers to cost effective development and certification of avionics systems
    - evaluate software contributions to aviation accidents
  - investigate alternate certification approaches
  - establish effective means for collaboration and transfer technology

We Need Your Help



- We want to better understand the technical challenges in developing and certifying avionics systems
  - What's eating your lunch? (*Thurs., 10:45am*)
- We want to know how to better interact with you
- We want to know how to better collaborate on research projects and transfer technology

In the end…



- We want to have a research program that will
  - develop technology to effectively and efficiently build and analyze software intensive systems
    - technology to verify that a software system satisfies all its requirements and maintains all its safety properties
    - technology to reduce the resources needed to certify flight-critical software
    - technology to effectively diagnose software contributions to aircraft accidents
- We hope that you can help us!